MOTOROLA

Law Department

June 18, 2012

Chief Judge Wolf
U.S. District Court
Moakley Courthouse
Boston, MA 02210

RE: United States v. Ryan Harris (09-10243-MLW).

Cable modem hacking impact to Motorola – June 2, 2012

Motorola first started designing its SURFboard® cable modems in the late 1990s with more than 75 million units sold as of 3Q 2011. Today, we remain the largest supplier of cable modems in the world, selling to cable operators and directly to the end consumer via traditional brick-and-mortar retail stores and online channels. Motorola and the SURFboard® cable modem have a reputation in the industry as being the most reliable, secure and interoperable solution – deployed on virtually every single Hybrid Fiber Coaxial (HFC) plant in the world. Unfortunately, this also factors into the SURFboard® cable modem becoming the target of hackers who want to modify it for the purpose of stealing Internet service from cable operators.

In the early 2000s, Motorola became aware of a hacking method on its SURFboard® cable modems which removed the bandwidth cap that was set by the cable operator. This allowed the hacker more bandwidth (i.e. faster connection to the Internet) without increasing their bill. This hacking method prompted cable operators to contact Motorola, claiming the SURFboard® cable modem was no longer secure and they would stop buying it. After hundreds of hours investigating the hacking method, Motorola discovered it was the Data Over Cable Service Interface Specification (DOCSIS®) that was being hacked and that all cable modems, not just Motorola's, were susceptible. In addition to educating the cable operators on this finding, Motorola then spent the next several years working with CableLabs (owner of DOCSIS and its certification process) ensuring improvements to the specification which prevented the uncapping hacking method on all cable modems – not just the SURFboard® cable modems.

In the mid 2000s, Motorola became aware of another hacking method on its SURFboard® cable modems which "cloned" the modem's identity (i.e. MAC address) – which allowed the hacker to create modems that were duplicates of authorized modems and steal Internet service from the cable operator. As this hacking method became more widespread, cable operators contacted Motorola again claiming the SURFboard® cable modem was no longer secure and they would stop buying it. As before, Motorola spent hundreds of hours investigating the hacking method and educating the cable operators it was DOCSIS® being hacked again-and that all cable modems, not just Motorola's, were susceptible. In addition

Motorola Mobility
600 North US Highway 45, Libertyville, IL 60048
Phone: (847) 523-5000

to working with CableLabs to improve the specification, Motorola also took steps to change the design of its SURFboard® cable modems to make them even more secure and resilient to the cloning hacking method.

In addition to the time spent investigating, educating the cable operators, working with CableLabs, and making design changes, Motorola's reputation and the SURFboard® brand have been damaged by these hacking attempts. Numerous press articles have appeared over the years reporting the hacking phenomenon against the SURFboard® cable modem which resulted in a diminished value for the brand. Motorola has spent hundreds of hours responding to these articles and protecting the reputation of the SURFboard® cable modem.

While Motorola has remained the world's largest supplier of cable modems, it has not come without significant effort and cost to counter these hacking methods. Ultimately, Motorola treats product security and reliability as priority number one, and we will continue to do so with core product lines, such as the SURFboard® cable modem.

Sincerely,

Chris Kohler
Motorola Mobility